Název práce: Důkazy s nulovou znalostí
Autor: Martin Primas
Katedra: Katedra Algebry
Vedoucí bakalářské práce: Doc. RNDr. Jiří Tůma, DrSc.
e-mail vedoucího: TUMA@karlin.mff.cuni.cz

Abstrakt: V předložené práci se věnujeme důkazum s nulovou znalostí. Pro definice důkazu s nulovou znalostí je použita teorie Turingových strojů, kterou ve stručnosti popíšeme na začátku práce. Na základě této teorie definujeme interaktivní důkazový systém a třídu jazyku, pro které tento systém existuje. Tato třída je zde podrobněji zkoumána. Dále předložíme různé definice důkazu s nulovou znalostí založené na této třídě a budeme hlouběji studovat jejich vzájemné vztahy. Formálním studiem těchto vztahů je tato práce nevšední. V práci rovněž uvedeme konkrétní příklady protokolu, u kterých dokážeme, že jde o důkazy s nulovou znalostí. V průběhu práce jsou definovány různé pojmy z teorie složitosti, které je na daném místě potřeba použít.

Klíčová slova: důkazy s nulovou znalostí, PZK, CZK, SZK

Title: Zero-knowledge proofs
Author: Martin Primas
Department: The Department of Algebra
Supervisor: Doc. RNDr. Jiří Tůma, DrSc.
Supervisor's e-mail address: TUMA@karlin.mff.cuni.cz

Abstract: This study presents findings on zero-knowledge proofs. At the beginning of this paper there is a brief description of the theory of Turing machines which is further used in definitions of zero-knowledge. Interactive proof system is defined on the basis of this theory as well as a class of all the languages for which the system exists. The class is thoroughly examined then. Next, various definitions of zero-knowledge proofs based on the class are presented and their mutual relations are investigated. It is just this formal investigation of these relations that makes this paper unique. Some concrete examples of protocols are also given and then proven to represent zero-knowledge proofs. Various terms of complexity theory are defined when needed within this study, too.

Keywords: zero-knowledge proofs, PZK, CZK, SZK